1. Teil: Lineare Algebra

1.1. Ein wenig über Gruppen und Ringe

Bemerkung: In diesem Abschnitt werden einige Begriffe und Resultate aus der Algebra wiederholt, die später verwendet werden.

Def.: Es sei $G \neq \emptyset$ eine Menge und $\cdot$ eine Verknüpfung auf G (d.h. eine Abbildung $\cdot : G \times G \to G$, $(a,b) \mapsto a \cdot b$. Gelten die Eigenschaften

1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a,b,c \in G$ (Assoziativität)
2) $\exists e \in G$ $\forall a \in G$: $e \cdot a = a \cdot e = a$ (neutrales Element)
3) $\forall a \in G$ $\exists a^{-1} \in G$: $a \cdot a^{-1} = a^{-1} \cdot a = e$ (inverses Element)

so wird $(G, \cdot)$ eine Gruppe genannt.

Def.: Es sei $(G, \cdot)$ eine Gruppe. Gilt zusätzlich

4) $a \cdot b = b \cdot a$ $\forall a,b \in G$ (Kommutativität)

so wird $(G, \cdot)$ eine abelsche (oder kommutative) Gruppe genannt.

Bemerkungen: 1) In der Voraussetzung, dass $\cdot$ eine Verknüpfung ist, ist die Abgeschlossenheit von G bezüglich $\cdot$ enthalten. D.h. in einer Gruppe ist stets $a \cdot b \in G$ $\forall a,b \in G$ erfüllt. Ist das nicht klar, muss man es überprüfen (und wird oft in den Gruppenaxiomen angegeben).

2) Die Verknüpfung $\cdot$ wird oft nicht geschrieben, d.h. man schreibt ab statt $a \cdot b$.

3) Die Verknüpfung wird (besonders bei abelschen Gruppen) oft $+$ geschrieben, d.h. man schreibt $a+b$ statt $a \cdot b$. Das neutrale Element wird dann meistens als 0 und das Inverse zu a als $-a$ geschrieben. D.h. die Gruppenaxiome der (abelschen) Gruppe $(G, +)$ sind

1) $(a+b)+c = a+(b+c)$ $\forall a,b,c \in G$ (Assoziativität)
2) $\exists 0 \in G$ $\forall a \in G$: $0+a = a+0 = a$ (neutrales Element)
3) $\forall a \in G$ $\exists -a \in G$: $-a+a = a+(-a) = 0$ (inverses Element)
4) $a+b = b+a$ $\forall a,b \in G$ (Kommutativität)

4) Ist die Verknüpfung klar, so schreibt man oft nur G statt $(G, \cdot)$.

Bspe.: 1) $(\mathbb{Z}, +)$ ist abelsche Gruppe

2) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind abelsche Gruppen

3) Allgemein gilt: Ist $(K, +, \cdot)$ ein Körper, so ist $(K, +)$ eine abelsche Gruppe (nach der Definition eines Körpers)

4) $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{C}\setminus\{0\},\cdot)$ sind abelsche Gruppen

5) Allgemein gilt: Ist $(K,+,\cdot)$ ein Körper, so ist $(K\setminus\{0\},\cdot)$ eine abelsche Gruppe.

6) Versieht man $\mathbb{R}^2=\left\{\begin{pmatrix}x\\y\end{pmatrix} \,\middle|\, x,y\in\mathbb{R}\right\}$ mit der Addition $\begin{pmatrix}x_1\\y_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\end{pmatrix}:=\begin{pmatrix}x_1+x_2\\y_1+y_2\end{pmatrix}$

(komponentenweise Addition von Vektoren), so ist $(\mathbb{R}^2,+)$ eine abelsche Gruppe

- Abgeschlossenheit: $\begin{pmatrix}x_1+x_2\\y_1+y_2\end{pmatrix}\in\mathbb{R}^2 \quad \forall \begin{pmatrix}x_1\\y_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\end{pmatrix}\in\mathbb{R}^2$
- Assoziativität: $\left(\begin{pmatrix}x_1\\y_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\end{pmatrix}\right)+\begin{pmatrix}x_3\\y_3\end{pmatrix}=\begin{pmatrix}(x_1+x_2)+x_3\\(y_1+y_2)+y_3\end{pmatrix}=\begin{pmatrix}x_1+(x_2+x_3)\\y_1+(y_2+y_3)\end{pmatrix}=\begin{pmatrix}x_1\\y_1\end{pmatrix}+\left(\begin{pmatrix}x_2\\y_2\end{pmatrix}+\begin{pmatrix}x_3\\y_3\end{pmatrix}\right)$

  für alle $\begin{pmatrix}x_1\\y_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\end{pmatrix},\begin{pmatrix}x_3\\y_3\end{pmatrix}\in\mathbb{R}^2$
- neutrales Element: $\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}+\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix} \quad \forall \begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$
- inverses Element: $\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}-x\\-y\end{pmatrix}=\begin{pmatrix}-x\\-y\end{pmatrix}+\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix} \quad \forall \begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$
- Kommutativität: $\begin{pmatrix}x_1\\y_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\end{pmatrix}=\begin{pmatrix}x_1+x_2\\y_1+y_2\end{pmatrix}=\begin{pmatrix}x_2+x_1\\y_2+y_1\end{pmatrix}=\begin{pmatrix}x_2\\y_2\end{pmatrix}+\begin{pmatrix}x_1\\y_1\end{pmatrix} \quad \forall \begin{pmatrix}x_1\\y_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\end{pmatrix}\in\mathbb{R}^2$

7) Versieht man $\mathbb{R}^3=\left\{\begin{pmatrix}x\\y\\z\end{pmatrix} \,\middle|\, x,y,z\in\mathbb{R}\right\}$ mit der Addition $\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}+\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}:=\begin{pmatrix}x_1+x_2\\y_1+y_2\\z_1+z_2\end{pmatrix}$

(komponentenweise Addition von Vektoren), so ist $(\mathbb{R}^3,+)$ eine abelsche Gruppe

<u>Notation</u> Wir verwenden in dieser Vorlesung die Bezeichnung $\mathbb{N}^+=\mathbb{N}\setminus\{0\}=\{1,2,3,\dots\}$ (mit $\mathbb{N}=\{0,1,2,3,\dots\}$ wie in der Schule üblich).

8) Es sei $n\in\mathbb{N}^+$. Versieht man $\mathbb{R}^n=\left\{\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix} \,\middle|\, x_1,\dots,x_n\in\mathbb{R}\right\}$ mit der komponentenweisen Addition $\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}+\begin{pmatrix}y_1\\\vdots\\y_n\end{pmatrix}:=\begin{pmatrix}x_1+y_1\\\vdots\\x_n+y_n\end{pmatrix}$, so ist $(\mathbb{R}^n,+)$ eine abelsche Gruppe

9) Es sei $n\in\mathbb{N}^+$ und K ein Körper. Dann gilt allgemein: Versieht man $K^n=\left\{\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix} \,\middle|\, x_1,\dots,x_n\in K\right\}$ mit der komponentenweisen Addition $\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}+\begin{pmatrix}y_1\\\vdots\\y_n\end{pmatrix}:=\begin{pmatrix}x_1+y_1\\\vdots\\x_n+y_n\end{pmatrix}$, so ist $(K^n,+)$ eine abelsche Gruppe.

10) Es sei $G=\{1,-1\}$ ($\subseteq\mathbb{Z}$), versehen mit der üblichen Multiplikation ganzer Zahlen, also mit Verknüpfungstafel

$\cdot$	1	-1
1	1	-1
-1	-1	1

, so ist $(G,\cdot)$ eine abelsche Gruppe.

Abgeschlossenheit ist klar, Assoziativität gilt, da sie auf $\mathbb{Z}$ gilt, neutrales Element ist 1, $1^{-1}=1$ und $(-1)^{-1}=-1$. Kommutativität gilt, da sie auf $\mathbb{Z}$ gilt

1.10.2024

Lemma 1 Es sei $(G,\cdot)$ eine Gruppe

(i) Das neutrale Element von G ist eindeutig bestimmt,

(ii) Das inverse Element jedes Gruppenelements $a \in G$ ist eindeutig bestimmt.

Beweis: (i) Sind $e,f \in G$ neutrale Elemente, so $e = e \cdot f = f$

(ii) Sind $x,y \in G$ inverse Elemente zu a, so $a \cdot x = x \cdot a = e = a \cdot y = y \cdot a$

$\Longrightarrow x = x \cdot e = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$

Bemerkung: Lemma 1 (ii) rechtfertigt die Notation a^{-1} für das inverse Element von a

Lemma 2 Es sei $(G,\cdot)$ eine Gruppe

(i) $(a^{-1})^{-1} = a \quad \forall a \in G$,

(ii) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall a,b \in G$

Beweis: (i) Da $aa^{-1} = a^{-1}a = e$ folgt $(a^{-1})^{-1} = a$ aus Lemma 1 (ii)

(ii) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ und analog $(b^{-1}a^{-1})(ab) = e$

Die Beh. folgt aus Lemma 1 (ii).

Bemerkung: In einer abelschen Gruppe $(G,+)$ wird Lemma 2 zu $-(-a) = a \quad \forall a \in G$ und $-(a+b) = (-b)+(-a) \; (= (-a)+(-b)) \quad \forall a,b \in G$

Def.: Es sei $(G,\cdot)$ eine Gruppe, $a \in G$ und $n \in \mathbb{N}$. Man setzt $a^0 := e$ (mit $e \in G$ neutrales Element) und $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ mal}}$ für $n \geq 1$.

Lemma 3 Es sei $(G,\cdot)$ eine Gruppe und $a \in G$. Dann ist $(a^n)^{-1} = (a^{-1})^n \quad \forall n \in \mathbb{N}$.

Beweis: Induktion nach n. $n=0$: $(a^0)^{-1} = e^{-1} = e = (a^{-1})^0$

(und $n=1$: $(a^1)^{-1} = a^{-1} = (a^{-1})^1$). Schließlich ist

$$(a^{n+1})(a^{-1})^{n+1} = (a^n a)(a^{-1}(a^{-1})^n) = a^n(aa^{-1})(a^{-1})^n = a^n e (a^{-1})^n = a^n (a^{-1})^n \overset{IV}{=} e$$

und analog $(a^{-1})^{n+1}(a^{n+1}) = e$. Die Beh. folgt aus Lemma 1 (ii).

Def: Ist $(G,\cdot)$ eine Gruppe, $a \in G$ und $n \in \mathbb{N}^+$. Dann sei $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.

Bemerkung: Ist $(G,+)$ eine abelsche Gruppe, so werden diese Definitionen zu

$\underset{\in \mathbb{Z}}{0} \cdot a = \underset{\in G}{0}$, $\; na = \underbrace{a + \cdots + a}_{n \text{ mal}}$ für $n \geq 1$ und $(-n)a = -(na) = n(-a)$ für $n \geq 1$.

Satz 4 Es sei $(G,\cdot)$ eine Gruppe

(i) $a^m a^n = a^{m+n} \quad \forall a \in G \; \forall m,n \in \mathbb{Z}$,

(ii) $(a^m)^n = a^{mn} \quad \forall a \in G \; \forall m,n \in \mathbb{Z}$,

(iii) Ist G abelsch, ist $(ab)^n = a^n b^n \quad \forall a,b \in G \; \forall n \in \mathbb{Z}$.

Der Beweis ist technisch (Induktion, Fallunterscheidungen) und wird ausgelassen

Bemerkung: Ist $(G,+)$ abelsch, so wird Satz 4 zu

(i) $ma + na = (m+n)a \quad \forall a \in G \; \forall n,m \in \mathbb{Z}$

(ii) $n(ma) = (nm)a \quad \forall a \in G \; \forall n,m \in \mathbb{Z}$

(iii) $n(a+b) = na + nb \quad \forall a,b \in G \; \forall n \in \mathbb{Z}$

Def.: Es sei $R \neq \emptyset$ eine Menge und $+$ und $\cdot$ zwei Verknüpfungen auf R (d.h. zwei Abbildungen $+ : R\times R \to R, (a,b) \mapsto a+b$ und $\cdot : R \times R \to R, (a,b)\mapsto a\cdot b$.
Gelten die Eigenschaften

1) $(R,+)$ ist eine abelsche Gruppe,

2) $(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall a,b,c\in R$ (Assoziativität der Multiplikation)

3) $a\cdot(b+c) = a\cdot b + a\cdot c$ und $(a+b)\cdot c = a\cdot c + b\cdot c \quad \forall a,b,c\in R$ (Distributivgesetze)

so wird $(R,+,\cdot)$ ein Ring genannt. Gilt zusätzlich (zu 1),2),3))

4) $\exists 1\in R \ \forall a\in R: 1\cdot a = a\cdot 1 = a$ (Existenz des Einselements)

so wird $(R,+,\cdot)$ Ring mit Einselement (oder Ring mit 1) genannt.
Gilt zusätzlich (zu 1),2),3))

5) $a\cdot b = b\cdot a \quad \forall a,b\in R$ (Kommutativität der Multiplikation)

so wird $(R,+,\cdot)$ ein kommutativer Ring genannt.
Gelten alle fünf Bedingungen 1)-5), so wird $(R,+,\cdot)$ kommutativer Ring mit 1 genannt.

Bemerkungen: 1) Auch bei Ringen ist die Abgeschlossenheit (d.h. $a+b\in R \ \forall a,b\in R$ und $a\cdot b\in R \ \forall a,b\in R$) darin enthalten, dass $+$ und $\cdot$ Verknüpfungen sind (und muss überprüft werden, wenn es nicht klar ist).

2) Auch bei Ringen schreibt man oft ab statt $a\cdot b$

3) Da $(R,+)$ eine abelsche Gruppe ist, verwendet man die dafür üblichen Bezeichnungen. Insbesondere wird das neutrale Element der Addition als 0 geschrieben (und Nullelement von R genannt) und das additive Inverse von $a\in R$ als $-a$ geschrieben.

4) Ebenso gelten alle für abelsche Gruppen gemachten Aussagen für $(R,+)$

5) Sind die Verknüpfungen klar, so schreibt man nur R (statt $(R,+,\cdot)$).

Notation: Ist $(R,+,\cdot)$ ein Ring und $a,b\in R$, so schreibt man $a-b := a+(-b)$.

Lemma 5 Es sei $(R,+,\cdot)$ ein Ring

(i) $0\cdot a = a\cdot 0 = 0 \quad \forall a\in R$ (wobei stets $0\in R$ gemeint ist),

(ii) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b) \quad \forall a,b\in R$,

(iii) $(-a)\cdot(-b) = a\cdot b \quad \forall a,b\in R$,

(iv) $a\cdot(b-c) = a\cdot b - a\cdot c$ und $(a-b)\cdot c = a\cdot c - b\cdot c \quad \forall a,b,c\in R$,

(v) $(na)b = a(nb) = n(ab) \quad \forall n\in\mathbb{Z} \ \forall a,b\in R$

(ohne Beweis)

Bspe.: 1) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer Ring mit 1

2) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ sind kommutative Ringe mit 1

3) Ist allgemein $(K,+,\cdot)$ ein Körper, so ist $(K,+,\cdot)$ ein kommutativer Ring mit 1
(Wir haben den Körperbegriff vorausgesetzt, könnten aber auch definieren: Ein Körper $(K,+,\cdot)$ ist ein kommutativer Ring mit 1, in dem $0\neq 1$ und jedes $a\in K\setminus\{0\}$ ein multiplikatives Inverses besitzt.)

<u>Def.</u>: Es sei $(R,+,\cdot)$ ein Ring mit 1. Ein $a\in R$ heißt invertierbar (oder Einheit), wenn $\exists a^{-1}\in R$ mit $a\cdot a^{-1}=a^{-1}\cdot a=1$. Das Element $a^{-1}\in R$ wird als Inverses von a bezeichnet.

<u>Lemma 6</u> Es sei $(R,+,\cdot)$ ein Ring mit 1

(i) Das Einselement $1\in R$ ist eindeutig bestimmt,

(ii) Ist $a\in R$ invertierbar, so ist das inverse Element von a eindeutig bestimmt.

<u>Beweis</u>: Analog zu Lemma 1

<u>Lemma 7</u> Es sei $(R,+,\cdot)$ ein Ring mit 1

(i) Ist $a\in R$ invertierbar, so ist auch $a^{-1}\in R$ invertierbar und $(a^{-1})^{-1}=a$,

(ii) Sind $a,b\in R$ invertierbar, so ist auch $a\cdot b\in R$ invertierbar und $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$

<u>Beweis</u>: Analog zu Lemma 2

<u>Def.</u>: Es sei $(R,+,\cdot)$ Ring mit 1, $a\in R$ und $n\in\mathbb{N}$. Dann sei $a^0:=1$ und $a^n=\underbrace{a\cdot\ldots\cdot a}_{n\text{mal}}$ für $n\geq 1$.

<u>Def.</u>: Es sei $(R,+,\cdot)$ ein Ring mit 1, $a\in R$ invertierbar und $n\in\mathbb{N}^+$. Dann sei $a^{-n}:=(a^n)^{-1}=(a^{-1})^n$
(Die Gleichung $(a^n)^{-1}=(a^{-1})^n$ zeigt man wie in Lemma 3.)

<u>Lemma 8</u> Es sei $(R,+,\cdot)$ ein Ring mit 1

(i) $a^n a^m=a^{m+n}$ $\forall a\in R$ $\forall m,n\in\mathbb{N}$,

(ii) $(a^m)^n=a^{mn}$ $\forall a\in R$ $\forall m,n\in\mathbb{N}$,

(iii) Ist R kommutativ, so ist $(ab)^n=a^n b^n$ $\forall a,b\in R$ $\forall n\in\mathbb{N}$

<u>Beweis</u>: Analog zu Satz 4

<u>Lemma 9</u> Es sei $(R,+,\cdot)$ ein Ring mit 1

(i) Ist $a\in R$ invertierbar, so ist $a^m a^n=a^{m+n}$ $\forall m,n\in\mathbb{Z}$,

(ii) Ist $a\in R$ invertierbar, so ist $(a^m)^n=a^{mn}$ $\forall m,n\in\mathbb{Z}$,

(iii) Ist R kommutativ und $a,b\in R$ invertierbar, so ist $(ab)^n=a^n b^n$ $\forall n\in\mathbb{Z}$

<u>Beweis</u>: Analog zu Satz 4

2.10.2024

<u>Notation</u> Ist $(R,+,\cdot)$ ein Ring mit 1, so bezeichne $R^*:=\{a\in R\mid a \text{ ist invertierbar}\}$.

<u>Lemma 10</u> Ist $(R,+,\cdot)$ ein Ring mit 1, so ist $(R^*,\cdot)$ eine Gruppe

<u>Beweis</u>: $R^*\neq\emptyset$, da $1\in R$ (aus $1\cdot1=1$ folgt $1^{-1}=1$). Abgeschlossenheit folgt aus Lemma 7 (ii), Assoziativität gilt, da sie für den Ring $(R,+,\cdot)$ gilt, $1\in R^*$ ist neutrales Element und inverse Elemente existieren wegen Lemma 7 (i).

Bsp.: 1) $\mathbb{Z}^* = \{-1, 1\}$

2) $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ und $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

3) Ist allgemein $(K, +, \cdot)$ ein Körper, so ist $K^* = K \setminus \{0\}$

Bemerkung: Die Bezeichnung R^* ist in der Algebra üblich, stimmt mit der in der Schule üblichen aber nur überein, wenn R ein Körper ist. Beachten Sie, dass $\mathbb{Z}^*$ in der Schule üblicherweise eine andere Bedeutung hat und die Bezeichnung $\mathbb{N}^*$ hier sinnlos ist, da $(\mathbb{N}, +, \cdot)$ kein Ring ist.

Def.: Ist $(R, +, \cdot)$ ein Ring mit 1, so wird $(R^*, \cdot)$ als Einheitengruppe von R bezeichnet.